Aula 03

FATORAÇÃO ÚNICA E CONGRUÊNCIAS

META

Apresentar a estrutura de domínio fatorial e estabelecer o conceito de congruência em $\mathbb{Z}$.

OBJETIVOS

Definir número inteiro primo bem como reconhecer suas propriedades básicas.
Aplicar o teorema fundamental da Aritmética na demonstração de propriedades relativas à fatoração em $\mathbb{Z}$.
Definir congruência e aplicar, mas propriedades na resolução de problemas de Aritmética.

PRÉ-REQUISITOS

O curso de Fundamento de Matemática e os conteúdos discutidos nas duas primeiras aulas.

INTRODUÇÃO

Olá, caro aluno! Estamos aqui, mais uma vez. Espero que você tenha compreendido todos os conteúdos discutidos nas aulas anteriores, pois a compreensão desta aula e de diversos tópicos das aulas futuras depende do conhecimento desses conteúdos.

Dividimos esta aula em duas partes onde, na primeira discutiremos a estrutura de domínio fatorial dos inteiros, definindo número primo e estabelecendo suas primeiras propriedades. Na segunda parte, estabeleceremos a relação da congruência em $\mathbb{Z}$, apresentando as propriedades da divisibilidade de um modo bastante simples. Finalizaremos a aula, aproveitando o fato da relação de congruência ser uma relação de equivalência em $\mathbb{Z}$ e apresentando a estrutura de anel comutativo das classes residuais.

FATORAÇÃO ÚNICA

Definição 1. Dizemos que um inteiro p é primo se $p \notin \{-1,0,1\}$ e toda vez que p divide um produto ele divide um dos fatores.

Exemplo 1. O inteiro 6 não é primo. Notemos que embora $6 \notin \{-1,0,1\}$, 6 divide $12 = 3.4$, 6 não divide 3 e nem divide 4. O número 5 é primo, pois $5 \notin \{-1,0,1\}$ e sempre que $5|ab$ com a e b inteiros, a ou b é múltiplo de 5.

Proposição 1. Seja $p \in \mathbb{Z}\backslash\{-1,0,1\}$. Uma condição necessária e suficiente para que p seja primo é que seu conjunto de divisores seja $\{-p,-1,1,p\}$.

Demonstração: (Suficiência). Sejam $p,a,b \in \mathbb{Z}$ com p primo e $p = ab$. Segue que $p|ab$, logo, $p|a \;\; ou \;\; p|b$. Se $p|a$, existe $a' \in \mathbb{Z}$ tal que $a = pa'$ e neste caso temos $p = pa'b$ que implica $a'b = 1$ e conseqüentemente $b = \pm 1$ e $a = \pm p$. Se, $p|b$, analogamente existe $b' \in \mathbb{Z}$ tal que $p = pb'$ e $p = apb'$ donde temos $a = \pm 1$ e $b = \pm p$. Portanto, o conjunto dos divisores de p é $\{-p,-1,1,p\}$.

(Necessidade). Suponhamos que o conjunto dos divisores de p seja $\{-p,-1,1,p\}$ e que $p|ab$ onde $a,b \in \mathbb{Z}$. Vamos provar que $p|a \;\; ou \;\; p|b$. Com efeito, se $p \nmid a$, do fato de que os únicos divisores de p são $-p,-1,1$ e p e que $mdc(a,p) > 0$, temos que $mdc(a,b) = 1$. Logo existem $r,s \in \mathbb{Z}$ tais que $pr + as = 1$ e por conseguinte, $bps + abr = b$.como $p|bps$ e $p|abr$, segue que $p|b$.

Observação: Notemos que todo $a \in \mathbb{Z}$ admite $-a,-1,1,a$ como divisores. Estes são os chamados divisores triviais de a. Se $|a| > 1$ e a não é primo além dos divisores triviais, a tem outros divisores, chamados divisores próprios.

Exemplo 2. Os divisores de -6 são $-6,-3,-2,-1,1,2,3$ e 6. Os números $-3,-2,2$ e 3 são os divisores próprios de 6.

Um inteiro não nulo que tem divisores próprios é comumente chamado composto.

Proposição 2. (Teorema fundamental da Aritmética). Todo inteiro $a, a \geq 2$ Pode ser escrito na forma

$$a = p_1.p_2 \ldots .p_r \qquad (\star)$$

onde $r \geq 1$ e $p_1,p_2,\ldots,p_r$ são inteiros primos positivos não necessariamente distintos. Além disto, a expressão $(\star)$, a menos da ordem dos fatores é única.

Demonstração: Vamos inicialmente provar a existência da expressão $(\star)$, usando indução em a.

Para $a = 2$; temos $r = 1$ e $p_1 = 2$ ou seja $a = p_1$ ok!

Seja $a \in \mathbb{Z}$ $a > 2$ e suponhamos que $\forall\, b \in \mathbb{Z}$, $2 \leq b < a$, b passar ser escrito como um produto de primos e, usando este fato, vamos provar que o mesmo acontece com a. Se a é primo ok! ($a = p_1 \quad (r = 1)$) e, se a não é primo, existem $b_1, b_2 \in \mathbb{Z}$, com $2 \leq b_1, b_2 < a$ e $b_1.b_2 = a$. Como por hipótese de indução $b_1\ e\ b_2$ podem ser escrito na forma $(\star)$, segue que $a = \ b_1 b_2$ também pode. Portanto, todo inteiro maior do que 1 pode ser escrito na forma $(\star)$.

Quanto à unicidade, dado $a \in \mathbb{Z}, a > 2$, suponhamos que

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_s \qquad (1)$$

Onde $r, s \geq 1$ e $p_1, \dots, p_{r,} q_1, \dots, q_s$ são inteiros primos positivos, não necessariamente distintos. Vamos provar que $r = s$ e que após uma reordenação (se necessário), $p_1 = q_1, \dots, p_r = q_r$. Com efeito, como p_1 é primo e $p_1 | q_1 q_2 \dots q_s$ segue que $\exists\ j \in \{1,2, \dots, s\}$ tal que $p_1 | q_s$ (como atividade, usando a definição de primo e indução, prove isto). Após uma reordenação (se necessária), podemos supor que $d = 1$ e da expressão 1 temos que

$$p_2 p_2 \dots p_r = q_2 q_3 \dots q_s \qquad (2)$$

Sendo p_2 primo e como $p_2 | q_2. \dots .q_s$, segue que $p_2 | q_j$ para algum $j \in \{2, \dots, s\}$.
Como antes, podemos assumir $j = 1$ e a expressão 2 nos leva a

$$p_3 \dots p_r = q_3 \dots q_s \qquad (3)$$

Prosseguindo de modo análogo e supondo, que $r < s$,chegaremos à expressão

$$1 = q_{r+1}. \dots .q_s \qquad (4)$$

que é, um absurdo, pois nenhum primo divide 1. Portanto, $r \geq s$.
Também, se fosse $r > s$, de 1, chegaríamos a uma expressão do tipo

$$\mathrm{p_s} + 1 \dots . . \mathrm{p_r} = 1$$

o que seria absurdo.

Portanto, $r = s$ e, a menos da ordem dos fatores, $p_1 = q_1, \dots, p_r = q_r$, como queríamos demonstrar.

Observação: É fácil ver que no teorema fundamental da Aritmética, poderíamos ter tomado $a \in \mathbb{Z} \backslash \{-1,0,1\}$ e escrito $a = p_1, p_2, \dots, p_r$
onde $p_1, \dots p_r$ são primos positivos ou negativos, não necessariamente distintos.

Para $a \in \mathbb{Z}, a > 2$, a expressão

$$a = p_1^{n_1}.p_2^{n_2} \dots . . p_r^{n_r} \qquad (\star\star)$$

Onde $p_1, p_2. \dots . p_r$ são primos positivos tais que $p_1 < p_2 < \cdots < p_r$ e $m_1, m_2, \dots, m_r$ são inteiros positivos, é chamada fatoração canônica em primos positivos do inteiro a.

Vimos aqui que do ponto de vista da divisibilidade, os números primos são bastante simples, têm apenas quatro divisores e o teorema fundamental da Aritmética afirma que a menos de multiplicação por $1\ ou - 1$ e ordem dos fatores, todo inteiro pode ser escrito como um produto de números primos. Uma pergunta que você, caro aluno, pode fazer é a seguinte; para gerar todos os inteiros $\notin \{-1,0,1\}$, através de produtos precisamos de quantos números primos? Esta resposta é dada pela seguinte

Proposição 3. O conjunto dos números primos é infinito.

Demonstração: Vamos, por absurdo, supor que o conjunto dos números primos positivos seja finito. Digamos
$P = \{p_1 = 2, p_2 = 3, p_3, \dots, p_n\}$ e construamos o inteiro $a = p_1 p_2 \dots p_n + 1$. Do teorema fundamental da Aritmética existe um $p \in P$ tal que $p | a$ e como $p | p_1 p_2 \dots p_n$ segue que $p | 1$ (pois $1 = a - p_1 p_2 \dots p_n$). Temos então um absurdo. Portanto existem infinitos primos positivos e conseqüentemente, infinitos inteiros primos.

Observação. Os números primos é até hoje um conteúdo bastante estudado pelos matemáticos, por exemplo, a distribuição dos primos é tão irregular que você pode encontrar dois primos ímpares consecutivos e dado um natural $n \geq 1$, qualquer, a seqüência de n inteiros consecutivos $(n + 1)! + 2, (n + 1)! + 3, \dots, (n + 1)! + (n + 1)$ é fornada apenas por inteiros compostos.

Dado um inteiro cujo numeral indo-arábico tem muitos algarismos, decidir se o inteiro é primo ou não é até hoje uma tarefa bastante difícil.

CONGRUÊNCIAS

Definição 1. Seja $m \in \mathbb{Z}_{+}^{*}$. Dizemos que os inteiros a e b são congruentes módulo m se $a - b$ é um múltiplo de m e escrevemos $a \equiv b(mod\ m)$
Exemplo 1. $10 \equiv 15(mod\ 5)$, $-8 \equiv -1(mod\ 7)$, $99 \equiv 9(mod\ 10)$.
Notemos que $a \equiv b(mod\ m) \Leftrightarrow m|a - b$.
Negamos $a \equiv b(mod\ m)$ escrevendo $a \not\equiv b(mod\ m)$(neste caso, $m \nmid a - b$).
Proposição 1. Dados $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}_{+}^{*}$, são equivalentes:
i)$a \equiv b(mod\ m)$.
ii) Os inteiros a e b quando divididos por m deixam o mesmo resto.
Demonstração: i⟹ii. Existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que $a = mq_1 + r_1$, $b = mq_2 + r_2$ e $0 \leq r_1, r_2 < m$. Segue que $a - b = m(q_1 - q_2) + (r_1 - r_2) \Rightarrow r_1 - r_2 = (a - b) + m(q_2 - q_1)$.

Como $m|a - b$ temos que $m|r_1 - r_2$. Do fato de que $0 \leq r_1, r_2 < m$, segue que $-m \leq r_1 - r_2 < m$ e como conseqüência temos $r_1 - r_2 = 0$ ou $r_1 = r_2$.
ii⟹i. Existem $q_1, q_2, r \in \mathbb{Z}$ com $0 \leq r < m$ tais que $a = mq_1 + r$ e $b = mq_2 + r$. Então $a - b = m(q_1 - q_2) \Longrightarrow m|a - b$, ou seja, $a \equiv b(mod\ m)$.

Exemplo 2. Como $98 \equiv 132(mod\ 17)$ seguem que 98 e 132 quando divididos por 17 deixam o mesmo resto: $98 = 17.5 + 13$ e $132 \equiv 17.7 + 13$.

Proposição 2. Sejam $a, b, c, m, n \in \mathbb{Z}$ sendo $m, n \geq 1$. Valem:
i) $a \equiv a(mod\ m)$.
ii) $a \equiv b(mod\ m) \Longrightarrow b = a(mod\ n)$.
iii) $a \equiv b(mod\ m)\ e\ b \equiv c(mod\ m) \Longrightarrow a \equiv c(mod\ m)$.
iv) $a \equiv b(mod\ m)\ e\ c \equiv d(mod\ m) \Longrightarrow a + c \equiv b + d(mod\ m)$.
v) $a \equiv b(mod\ m)\ e\ c \equiv d(mod\ m) \Longrightarrow a.c \equiv b.c(mod\ m)$.
vi) $a \equiv b(mod\ m) \Longrightarrow a^n \equiv b^n(mod\ m)$.

Demonstração:
i) $m|a - a \Rightarrow a \equiv a(mod\ m)$.
ii) $a \equiv b(mod\ m) \Longrightarrow m|a - b \Longrightarrow m|b - a \Longrightarrow b \equiv a(mod\ m)$.
iii)$\mathrm{a \equiv b(mod\ m)\ e\ b \equiv c(mod\ m) \Longrightarrow m|a - b, b - c \Longrightarrow m|a - c \Longrightarrow a \equiv c(mod\ m)}$.
iv) Como $m|a - b, c - d$ temos que $m|((a + c) - (b + d))$ ou seja,$a + c \equiv b + d(mod\ m)$.
v) Novamente, $m|a - b, c - b$, logo existe $q, q' \in \mathbb{Z}$ tais que $a = b + mq\ \ e\ \ c = d + mq' \Longrightarrow ac = (b + mq)(d + mq') \Longrightarrow \exists\ n \in \mathbb{Z}$ tal que $ac = db + mn \Longrightarrow m|ac - bd$, ou seja $ac \equiv bd(mod\ m)$.
vi) Notemos que $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$ como $m|a - b$ segue que $m|a^n - b^n$, ou seja, $a^n \equiv b^n(mod\ m)$.

Exemplo 3. Vamos determinar o resto da divisão de 3^{50} por 26. Notemos que $3^3 = 27 \equiv 1(mod\ 26)$. Isto implica que $(3^3)^{\ 16} \equiv 1^{16}(mod\ 26)$ ou seja, que $3^{48} \equiv 1(mod\ 26)$. Como $3^2 \equiv 3^2(mod\ 26)$ segue que $3^{50} \equiv 3^2(mod\ 26)$. Assim, $3^{50}\ e\ 9$ quando divididos por 26 deixam o mesmo resto que evidentemente, é 9. Este exemplo mostra que a relação de congruência

torna as propriedades da divisibilidade facilmente manipuláveis tornando menos trabalhoso este tipo de cálculo.

Notemos que os itens i), ii) e iii) da proposição anterior mostraram que a relação de congruência módulo um inteiro positivo m é uma relação de equivalência no conjunto dos números inteiros.

Dados $m \in \{1, 2, 3, \dots\}$ e $a \in \mathbb{Z}$, a classe de a, módulo esta relação de congruência, é chamada classe residual de a módulo m e a indicamos por $\bar{a}$. Indicamos o conjunto quociente (destas classes) por $\mathbb{Z}_n$.

Proposição 3. Para cada $n \in \{1, 2, \dots\}$, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ onde a cardinalidade de $\mathbb{Z}_n$ é n.

Demonstração: Dado $a \in \mathbb{Z}$, do algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que $a = mq + r$ e $0 \leq r \leq m-1$. Segue daqui que $m|a-r$, ou seja, que $a \equiv r(mod\, m)$. Isto mostra que $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

Agora, sejam $r_1, r_2 \in \{0,1, \dots, n-1\}$. Se $\bar{r}_1 = \bar{r}_2$ então $r_1 \equiv r_2(mod\, m)$ de modo que $m|r_1 - r_2$ e lembrando que $r_1, r_2 \in \{0,1, \dots, m-1\}$, segue que $r_1 = r_2$. Portanto $\mathbb{Z}_n$ tem exatamente n classes residuais.

Vamos definir em $\mathbb{Z}_n$, duas operações uma adição e uma multiplicação pondo:
$\bar{a}, \bar{b} \in \mathbb{Z}_n, \bar{a} + \bar{b} = \overline{a+b}\ e\ \bar{a}.\bar{b} = \overline{ab}$.

Proposição 4. As operações de $\mathbb{Z}_n\, X\, \mathbb{Z}_n$ em $\mathbb{Z}_n$ de adição e multiplicação estabelecidas acima estão bem definidas. Ou seja, não dependem dos representantes das classes.

Demonstração: sejam $a' \in \bar{a}$ e $b' \in \bar{b}$. Então $a' \equiv a(mod\, m)$ e $b' \equiv b(mod\, m)$. Então $a' + b' \equiv a + b(mod\, m)$ donde temos que $\overline{a' + b'} = \overline{a+b}$.

Proposição 5. As operações de adição e de multiplicação acima definidas no conjunto $\mathbb{Z}_n$ verificam às seguintes propriedades:
i) $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})\ \forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
ii) $\bar{a} + \bar{c} = \bar{b} + \bar{a}\quad \forall \bar{a}, \bar{b}, \in \mathbb{Z}_n$
iii) $\exists\ \bar{o} \in \mathbb{Z}_n$ tal que $\bar{a} + \bar{o} = \bar{a}\quad \forall \bar{a} \in \mathbb{Z}_n$
iv) $\forall \bar{a} \in \mathbb{Z}_n, \exists - \bar{a}$ tal que $\bar{a} + (-\bar{a}) = \bar{0}$
v) $(\bar{a}\, .\, \bar{b}).\bar{c} = \bar{a}.(\bar{b}.\bar{c})\ \forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
vi) $\bar{a}.\bar{b} = \bar{b}.\bar{a}\quad \forall \bar{a}, \bar{b}, \in \mathbb{Z}_n$
vii) $\bar{a}.(\bar{b} + \bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}\ \forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
viii) $\exists \bar{1} \in \mathbb{Z}_n$ tal que $\bar{a}.\bar{1} = \bar{a}\ \ \forall \bar{a} \in \mathbb{Z}_n$

Demonstração: (será deixada como atividade)

Comentário $(\mathbb{Z}_n, +, .)$ munido das oito propriedades acima é um dos primeiros exemplos dos anéis comutativos finitos que estudaremos futuramente.

RESUMO

Caro aluno, nesta terceira aula discutimos inicialmente o conceito de número primo onde demonstramos o teorema fundamental da Aritmética e como primeira conseqüência deste teorema concluímos que existem infinitos números primos. Por fim, estabelecemos o conceito de congruência que é uma forma simples de apresentar propriedades da divisibilidade. Usando a relação de congruência em $\mathbb{Z}$ exibimos os anéis $\mathbb{Z}_n$ conhecidos também como os anéis das classes

de restos, construindo com isto um dos primeiros exemplos de anéis finitos, terminando com esta aula o estudo dos números inteiros necessário na composição dos pré-requisitos para as aulas futuras.

ATIVIDADES

1. Sejam $a = p_1^{m_1}.p_2^{m_2} \dots..p_r^{m_r}$ e b= $p_1^{n_1}.p_2^{n_2} \dots..p_r^{n_r} \in \mathbb{Z}$ onde $p_1, p_2, \dots, p_r$ são primos positivos distintos e $m_1, \dots, m_r, n_1, \dots, n_r \in \{0,1,2, \dots\}$. Se $k_i = \text{mín}\{m_i, n_i\}$ e $l_i = máx\{m_i, n_i\}$ prove que $mdc(a,b) = p_1^{k_1}. \dots .p_r^{k_r}$ e $mmc(a,b) = p_1^{l_1}. \dots .p_r^{l_r}$.

2. Seja $a \in \mathbb{Z}$, um número ímpar. Prove que $a \equiv -1(mod\ 4)$ ou $a \equiv 1(mod\ 4)$.

3. Sejam $a, b, c, m \in \mathbb{Z},\ m \geq 1$ onde $mdc(a,m) = 1$. Prove que se $b \equiv c(mod\ m)$ então $ab \equiv ac(mod\ m)$.

4. Sejam $a, b, c, \in \mathbb{Z}$ tais que a ou b é não nulo. Prove que a equação diofantina $ax + by = c$ tem solução se, e somente se, $mdc(a,b)|c$. Se (x_0, y_0) é uma solução, prove que todas as outras podem ser postas na forma $\left(x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t\right), t \in \mathbb{Z}$, onde $d = mdc(a,b)$.

5. Encontre todos os $x \in \mathbb{Z}$ tais que.
a) $3x \equiv 4(mod\ 5)$.
b) $6x + 3 \equiv 1(mod\ 10)$.

6. Seja $p \in \mathbb{Z}_+$ um primo e $1 \leq k < p$ um inteiro. Prove que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ é um múltiplo de p.

7. Prove que, se $p \in \mathbb{Z}_+$ é primo então $\forall a, b \in \mathbb{Z}$, $(a + b)^p \equiv a^p + b^p(mod\ p)$.

8. Prove que o conjunto $P = \{p \in \mathbb{Z}; p$ é primo e $p \equiv -1(mod\ 4)\}$ é infinito. Sugestão: negue esta afirmação exibindo $P = \{p_1, p_2, \dots, p_n\}$ e o número $a = 4p_1 \dots p_n - 1$. Observe que, produto de números do tipo $4q + 1$, também é deste tipo.

3.1. Comentários das atividades.

Na primeira atividade, você, caro aluno, deve ter notado que se um primo p divide $d = mdc(a,b)$, então, por transitividade o mesmo deve dividir também a e b. Além disto, sendo $d = mdc(a,b)$, se d' é outro divisor comum de a e b então $d'|d$. Segue que a ordem (expoente) de p em d deve ser a mínima entre as ordens de p em a e em b. Quanto ao mínimo múltiplo comum, cada primo divisor deste, deve ser um divisor de a ou de b. Além disto, você deve ter lembrado que qualquer outro múltiplo comum de a e b é também múltiplo do $mmc(a,b)$, logo todo primo divisor do $mmc(a,b)$ deve ter ordem igual à maior das ordens de p em a e em b

Na segunda atividade, você deve ter notado que o resto da divisão de a por 4 deve ser 1 ou 3 e que $3 = -1(mod\ 4)$.

Na terceira atividade, você deve ter observado que $m|a(b-c)$ e como o $mdc\ (a,m) = 1$, o resultado é imediato.

Na quarta atividade, se (x_0, y_0) é uma solução então você deve ter percebido facilmente que mdc $(a, b)|ax. + by$.. Reciprocamente, se $d = mdc\ (a, b)$ divide c,então existe $(x_1, y_1) \in \mathbb{Z}\ X\ \mathbb{Z}$ tal que $ax_1 + bx_1 = d$ donde temos que $a\left(x_1.\frac{c}{d}\right) + b\left(y.\frac{c}{d}\right) = c$ e $(x_0, y_0) = \left(\frac{x_1c}{d}, \frac{y_1c}{d}\right)$ é uma solução da equação

Por outro lado, supondo que (x_0, y_0) é uma solução, substituindo diretamente na equação x por $x_0 - \frac{b}{d}t$ e y por $y_0 + \frac{a}{d}t$ para cada $t \in \mathbb{Z}$ você deve ter visto claramente que se trata de uma solução. Finalmente, usando o fato de que (x_0, y_0) e (x_1, y_1) são duas soluções da equação foi fácil obter um $t \in \mathbb{Z}$ tal que $(x_1, y_1) = \left(x_0 - \frac{b}{d}t, y_0\frac{a}{d}t\right)$.

Na quinta atividade item a, você não deve ter tido dificuldades se notou que esta congruência é equivalente à equação $\overline{3}.\bar{x} = \overline{4}$ no anel $\mathbb{Z}_5.0$ onde temos que $\bar{x} = \overline{3}^{-1}.\overline{4} = \overline{2}.\overline{4} = \overline{8} = \overline{3}$ ou seja $x \equiv 3(mod\ 5)$. No item b, temos $6x \equiv -2(mod\ 10)$ ou equivalentemente, $3x \equiv -1(mod\ 5)$.

Na sexta atividade, você, caro aluno, deve ter notado que para $0 < k < p$, os fatores de $k!$ e de $p - k!$ são menores do que p.

Na sétima atividade, você deve ter usado o desenvolvimento do binômio de Newton e aplicado a sétima atividade.

Na oitava atividade nós já sugerimos uma opção para a solução e esperamos que você tenha desenvolvido com êxito.

Lembramos sempre que os tutores estão disponíveis.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).